UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/808,629	03/24/2004	Dennis Cox	062891.0638	6090

5073 7590 04/14/2009

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
04/14/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/808,629	COX ET AL.	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 02/23/2009, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

Claims 1-33 are presented for examination.

Response to Remarks/Arguments

2. Applicant's arguments, with respect to the rejection of the claims have been fully considered but they are not persuasive.

2.1 In response to Applicant argument that the Coley-Malkin combination of references do not teach or suggest requesting an acknowledgement from the initiator of the request, Examiner respectfully disagrees citing the citations previously provided which recites, "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall (7:16-19)" and "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request (7:41-59)." Additionally the Examiner cited column 8 lines 3-9, which recites, "Access request verification can include analysis of: source host machine and source user information; destination host machine and

destination user information; and/or time of day analysis." The Applicant cited only a portion of this citation, however the entire citation provides complete disclosure of the claim limitation. The disclosure here is of a user that is making a request which has certain verification requirements and then the disclosed firewall verifying the request by means of analysis reads upon the argued claim limitations.

Applicant has not overcome the rejection.

2.2 In response to Applicant argument that the Coley-Malkin combination of references do not teach or suggest steps taken beyond discarding a packet when the source address matched a known internal, the Examiner respectfully disagrees citing column 8 lines 3-4 which recites, "a reliable request may require only a minimum of verification before being connected" and column 6 lines 4-20 – "In a preferred embodiment, individual proxy agents are assigned to designated ports to monitor, respond to and verify incoming access requests (i.e., incoming packets) received on the port ... assigned proxy agent immediately verifies the access request before a connection is formed. Using simple verification checks, the proxy agent determines the authority of the access request, quickly and efficiently discarding unauthorized requests without unduly burdening system resources. If the access request is authorized, the assigned proxy agent opens, and thereafter manages, the port connection."

Applicant has not overcome the rejection

Claim Rejections – 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10, 15-21, 27-29 and 30-33 are rejected under 35 U.S.C. 103(a) as being disclosed by Coley et al. (US Patent No. 5,826,014 hereinafter Coley) in view of Malkin et al. (US Patent No. 6,061,650 hereinafter Malkin).

Regarding claims 1, Coley, discloses a method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

- receiving a request for connection from an initiator, over the public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- requesting an acknowledgment from the initiator of the request (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request.").

Coley is silent in determining whether the acknowledgment has been received within a predetermined amount of time and denying the request if the acknowledgment is not received within the predetermined amount of time, however Malkin does provide such a disclosure (5:21-27 – "In step 234, after sending the tunnel registration request, the RAS sets a retransmit time and expects a registration reply from the gateway within a predetermined period of time. The RAS will retransmit the request if a response is not received within the predetermined period of time. After a predetermined number of unsuccessful attempts, the RAS will terminate the PPP connection with the remote node").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to modify the disclosure of Coley with that of Malkin because both disclosures are directed towards network security, particularly within a remote access network. Malkin provides motivation for this combination in the recitation, to implement the mobile routing protocols, additional software needs to be loaded onto the remote node to enable the node to communication with its original network without having to change its network address. As a result, a user is burdened with installing the mobile protocol software on their computer system and testing it to be sure it operates properly. The need described here lends reason to combine these two references.

Regarding claim 2, Coley, discloses the method of claim 1, wherein the public network is the Internet (Figure 2 element 202).

Regarding claim 3, Coley, discloses the method of claim 2, wherein the routing device is a firewall providing access to the Internet (Figure 2 element 210).

Regarding claim 4, Coley, discloses the method of claim 1, further comprising processing the request if the acknowledgement is received (10:36-40 – "after a proxy successfully completes its set of one or more verification tests, the proxy agent initiates a connection request to the destination machine (and port) on behalf of the incoming access request.").

Regarding claim 5, Coley, discloses the method of claim 1, further comprising adding an IP address of the initiator to a cache of IP addresses if the acknowledgement is not received (9:32-45 – "Source address verification can be based on a check of the validity of on or more specific addresses, or, on a range of address values (e.g., the first octet has a value of between zero and 100). Such a check involves a determination of whether a host source address of an incoming packet comports with a list of authorized or unauthorized addresses, or is within a designated range. If the source address is not on the list, the packet is discarded. Referring back to FIG. 3, in the event that the external user 300

attempts to contact a network element behind the firewall 318, the proxy agent can check the source address of the host computer 302. If the proxy agent determines that the host computer 302 does not have an authorized address, the request originating from the host computer 302 is discarded." and 13:21-32 – " additional security feature that can be provided in the firewall system is a transaction log. Such a log gathers information associated with any access request message seeking to connect to or inquire about network elements residing behind the firewall. Information gathered in such a transaction log may include, but is not limited to, the source address (what is the identity of the machine from which the request originated), the IP address (which Internet port system did the request originate over), the destination address (who is the request trying to reach), time of access, and/or the identity of user (who is using the source machine).").

Regarding claim 6, Coley, discloses the method of claim 5, further comprising denying access through the routing device to any IP address on the cache of IP addresses (11:40-46 – "In the present exemplary scenario the access request message is further analyzed to determine whether the access request is being received during an authorized time period, such as a time of day (step 418). If the time of day during which the access request is received is not authorized, the connection request is denied (step 420). The time of day assessment can be tailored for specified users, source host machines, and/or IP addresses." and

13:12-20 – "Another aspect of a system in accordance with the invention is the use of aliases by the firewall when addressing machines residing behind the firewall. A machine behind the firewall can be addressed by the firewall according to an alias of its actual IP address. Hence, if a hacker is somehow able to tap the firewall, any addresses detected by the hacker corresponding to machines attached to the backside of the firewall will be fictitious.").

Regarding claim 7, Coley, discloses the method of claim 1, further comprising storing information about the initiator on a system log for analysis by the system administrator (11:47-50 – "A proxy agent also can assess whether user or user/password information is necessary to gain access (step 422). If not, the proxy agent can initiate the connection (step 424). If the information is required, the proxy agent prompts the user with an appropriately formatted message to enter a username and/or password information (step 426).").

Regarding claim 8, Coley, discloses the method of claim 1, further comprising storing information about the request for connection on a system log for analysis by the system administrator (11:7-20 - "Because the access request seeks to access a destination address residing behind the firewall 318, the access request message is presented to the firewall 318 (step 404). In accordance with an exemplary embodiment, a proxy agent running on the firewall 318 is assigned to the access request in accordance with a preliminary analysis of the port number

designation within the packet representing the access request (step 406). In this case, port number 80 (HTTP) would ordinarily be designated in the request. The assessment also can involve a determination of whether the service indicated by the port number comports with the contents of the request (step 408)." And 13:21-32 – " additional security feature that can be provided in the firewall system is a transaction log. Such a log gathers information associated with any access request message seeking to connect to or inquire about network elements residing behind the firewall. Information gathered in such a transaction log may include, but is not limited to, the source address (what is the identity of the machine from which the request originated), the IP address (which Internet port system did the request originate over), the destination address (who is the request trying to reach), time of access, and/or the identity of user (who is using the source machine).").

Regarding claim 9, Coley, is silent in disclosing determining if a prior request for an acknowledgement has been sent to an IP address associated with the initiator and been unacknowledged within a predetermined amount of time, if the acknowledgement is not received, however Malkin does provide such a disclosure (5:21-27 – "In step 234, after sending the tunnel registration request, the RAS sets a retransmit time and expects a registration reply from the gateway within a predetermined period of time. The RAS will retransmit the request if a response is not received within the predetermined period of time. After a

predetermined number of unsuccessful attempts, the RAS will terminate the PPP connection with the remote node").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to modify the disclosure of Coley with that of Malkin because both disclosures are directed towards network security, particularly within a remote access network. Malkin provides motivation for this combination in the recitation, to implement the mobile routing protocols, additional software needs to be loaded onto the remote node to enable the node to communication with its original network without having to change its network address. As a result, a user is burdened with installing the mobile protocol software on their computer system and testing it to be sure it operates properly. The need described here lends reason to combine these two references.

Regarding claim 10, Coley, discloses the method of claim 1, further comprising using diagnostic tools to determine additional information about a source of the request for connection (8:1-9 – "the source address of an access request can be investigated to determine whether the request is suspect or credible. An inherently reliable request may require only a minimum of verification before being connected. While a suspect request may require enhanced verification. Access request verification can include analysis of: source host machine and

source user information; destination host machine and destination user information; and/or time of day analysis.").

Regarding claim 15, Coley, discloses a method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

- receiving an incoming data packet from the public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- comparing a source address of the data packet against known internal addresses of the private network (9:6-19 and 32-46 – "investigation of a source address (i.e., the host machine from which the access inquiry originated) of the access request. This permits the proxy agent to make an initial assessment of the authenticity of the request … Once the source is determined, the proxy agent can run an appropriate combination of verification checks suited to the integrity of the request as indicated by its source");
- determining if the source address matches a known internal address (9:6-19 and 32-46 – "investigation of a source address (i.e., the host machine from which the access inquiry originated) of the access request. This permits the proxy agent to make an initial assessment of the authenticity of the request … Once the source is determined, the proxy agent can run

an appropriate combination of verification checks suited to the integrity of the request as indicated by its source")

Coley does however disclose:

- dropping the data packet (9:4-5 – "If there is a discrepancy, the request is denied");
- analyzing a header of the data packet (9:3-8 – "investigation of a source address (i.e., the host machine from which the access inquiry originated) of the access request. This permits the proxy agent to make an initial assessment of the authenticity of the request");
- determining information regarding a history of the packet (8:5-16 – "source address of an access request can be investigated to determine whether the request is suspect or credible … Access request verification can include analysis of: source host machine and source user information; destination host machine and destination user information; and/or time of day analysis");
- determining a real source of the data packet using the information regarding the history of the packet (8:5-16 – "source address of an access request can be investigated to determine whether the request is suspect or credible … Access request verification can include analysis of: source host machine and source user

information; destination host machine and destination user information; and/or time of day analysis"); and

- refusing to process any additional data packets received from the real source of the data packet (9:6-19 and 32-46 – "If there is a discrepancy, the request is denied").

Regarding claim 16, Coley, discloses the method of claim 15, further comprising storing data about the data packet on a system log, for use and analysis by a system administrator (Rejected under the same rational as claim 7).

Regarding claim 17, Coley, discloses the method of claim 15, wherein the public network is the Internet (Rejected under the same rational as claim 2).

Regarding claim 18, Coley, discloses the method of claim 17, wherein the routing device is a firewall providing access to the Internet (Rejected under the same rational as claim 3).

Regarding claim 19, Coley, discloses the method of claim 15, further comprising forwarding the data packet to the private network if there is not a match (Rejected under the same rational as claim 6).

Regarding claim 20, Coley, discloses the method of claim 15, further comprising adding an IP address of the data packet to a cache of IP addresses if there is a match (Rejected under the same rational as claim 6).

Regarding claim 21, Coley, discloses the method of claim 20, further comprising denying access through the routing device to any IP address on the cache of IP addresses (Rejected under the same rational as claim 6).

Regarding claim 27, Coley, discloses the method for blocking an attack on a private network implemented by a routing device interconnecting the private network to a public network, comprising:

- receiving a request for connection from an initiator, over the public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- requesting an acknowledgment from the initiator of the request (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request.");
- comparing a source address of the request for connection with known internal addresses of the private network (9:32-46);

- determining if the source address matches a known internal address (9:32-46); and refusing to process the request for connection if there is a match (9:32-46).

Coley is silent in determining whether the acknowledgment has been received within a predetermined amount of time and denying the request if the acknowledgment is not received within the predetermined amount of time, however Malkin does provide such a disclosure (5:21-27 – "In step 234, after sending the tunnel registration request, the RAS sets a retransmit time and expects a registration reply from the gateway within a predetermined period of time. The RAS will retransmit the request if a response is not received within the predetermined period of time. After a predetermined number of unsuccessful attempts, the RAS will terminate the PPP connection with the remote node").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to modify the disclosure of Coley with that of Malkin because both disclosures are directed towards network security, particularly within a remote access network. Malkin provides motivation for this combination in the recitation, to implement the mobile routing protocols, additional software needs to be loaded onto the remote node to enable the node to communication with its original network without

having to change its network address. As a result, a user is burdened with installing the mobile protocol software on their computer system and testing it to be sure it operates properly. The need described here lends reason to combine these two references.

Regarding claim 28, Coley, discloses system for blocking an attack on a private network, comprising: a routing device being operable to interconnect a private network to a public network, the routing device being further operable to: receive a request for connection from an initiator, over the public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall"); request an acknowledgment from the initiator of the request (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request.").

Coley is silent in determining whether the acknowledgment has been received within a predetermined amount of time and denying the request if the acknowledgment is not received within the predetermined amount of time, however Malkin does provide such a disclosure (5:21-27 – "In step 234, after sending the tunnel registration request, the RAS sets a retransmit time and expects a registration reply from the gateway within a

predetermined period of time. The RAS will retransmit the request if a response is not received within the predetermined period of time. After a predetermined number of unsuccessful attempts, the RAS will terminate the PPP connection with the remote node").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to modify the disclosure of Coley with that of Malkin because both disclosures are directed towards network security, particularly within a remote access network. Malkin provides motivation for this combination in the recitation, to implement the mobile routing protocols, additional software needs to be loaded onto the remote node to enable the node to communication with its original network without having to change its network address. As a result, a user is burdened with installing the mobile protocol software on their computer system and testing it to be sure it operates properly. The need described here lends reason to combine these two references.

Regarding claim 29, Coley, discloses system for blocking an attack on a private network, comprising:

- a routing device being operable to interconnect the private network and a public network, the routing device being further operable to: receive an incoming data packet from the public network (7:16-19 – "a user operating

a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");

- compare a source address of the data packet against known internal addresses of the private network (9:6-19 and 32-46);
- determine if the source address matches a known internal address (9:6-19 and 32-46); and if there is a match: drop the data packet (9:39);
- analyze a header of the data packet (9:3-8);
- determine information regarding a history of the packet (8:5-16);
- determine a real source of the data packet using the information regarding the history of the packet (8:5-16); and
- refuse to process any additional data packets received from the real source of the data packet (9:6-19 and 32-46).

Regarding claim 30, Coley, discloses a system for blocking an attack on a private network, comprising:

- means for interconnecting a private network to a public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- means for receiving a request for connection from an initiator, over the public network (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy

agent tailored to the particular protocol and verification requirements of that incoming access request.");

- means for requesting an acknowledgment from the initiator of the request (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request.");

Coley is silent in determining whether the acknowledgment has been received within a predetermined amount of time and means for denying the request if the acknowledgment is not received within the predetermined amount of time, however Malkin does provide such a disclosure (5:21-27 – "In step 234, after sending the tunnel registration request, the RAS sets a retransmit time and expects a registration reply from the gateway within a predetermined period of time. The RAS will retransmit the request if a response is not received within the predetermined period of time. After a predetermined number of unsuccessful attempts, the RAS will terminate the PPP connection with the remote node").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to modify the disclosure of Coley

with that of Malkin because both disclosures are directed towards network security, particularly within a remote access network. Malkin provides motivation for this combination in the recitation, to implement the mobile routing protocols, additional software needs to be loaded onto the remote node to enable the node to communication with its original network without having to change its network address. As a result, a user is burdened with installing the mobile protocol software on their computer system and testing it to be sure it operates properly. The need described here lends reason to combine these two references.

Regarding claim 31, Coley, discloses a system for blocking an attack on a private network, comprising:

- means for interconnecting the private network and a public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- means for receiving an incoming data packet from the public network; means for comparing a source address of the data packet against known internal addresses of the private network (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request.");

- means for determining if the source address matches a known internal address (9:6-19 and 32-46);

  and if there is a match:
- means for dropping the data packet (9:39 – "If there is a discrepancy, the request is denied");
- analyzing a header of the data packet (9:39);
- determining information regarding a history of the packet (8:5-16);
- determining a real source of the data packet using the information regarding the history of the packet (8:5-16); and
- refusing to process any additional data packets received from the real source of the data packet (9:6-19 and 32-46)

Regarding claim 32, Coley, discloses a software embodied in a computer-readable medium, the computer-readable medium comprising code operable to:

- interconnect a private network to a public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- receive a request for connection from an initiator, over the public network; request an acknowledgment from the initiator of the request (7:41-59 – "firewall 210 application assess the characteristics of an incoming request and assigns an appropriate proxy agent tailored to the particular protocol and verification requirements of that incoming access request.").

> Coley is silent in determining whether the acknowledgment has been received within a predetermined amount of time and denying the request if the acknowledgment is not received within the predetermined amount of time, however Malkin does provide such a disclosure (5:21-27 – "In step 234, after sending the tunnel registration request, the RAS sets a retransmit time and expects a registration reply from the gateway within a predetermined period of time. The RAS will retransmit the request if a response is not received within the predetermined period of time. After a predetermined number of unsuccessful attempts, the RAS will terminate the PPP connection with the remote node").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to modify the disclosure of Coley with that of Malkin because both disclosures are directed towards network security, particularly within a remote access network. Malkin provides motivation for this combination in the recitation, to implement the mobile routing protocols, additional software needs to be loaded onto the remote node to enable the node to communication with its original network without having to change its network address. As a result, a user is burdened with installing the mobile protocol software on their computer system and testing it to be sure it operates properly. The need described here lends reason to combine these two references.

Regarding claim 33, Coley, discloses a Software embodied in a computer-readable medium, the computer-readable medium comprising code operable to:

- receive an incoming data packet from the public network (7:16-19 – "a user operating a host machine 200 who attempts to access the internal network 214 via the public network 202 must go through the firewall");
- compare a source address of the data packet against known internal addresses of the private network (9:6-19 and 32-46);
- determine if the source address matches a known internal address (9:6-19 and 32-46);

  and if there is a match:
- drop the data packet (9:39); analyze a header of the data packet (9:3-8);
- determine information regarding a history of the packet (8:5-16);
- determine a real source of the data packet using the information regarding the history of the packet (8:5-16); and
- refuse to process any additional data packets received from the real source of the data packet (9:6-19 and 32-46).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11-14 and 2-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley -Malkin and further in view of Levinson et al. (US Application Publication No. 20030053170).

Regarding claim 11, Coley-Malkin, is silent in disclosing the method of claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using trace root diagnostic tools to determine information about the source of the request for connection, however Levinson et al. does disclose network tools used in the collection of additional information about a network (0008 – "network diagnostics"). It would have been obvious for one of ordinary skill in the art to modify the disclosed network diagnostic functions of Levinson et al. into the specific network diagnostic tools mentioned within the claim language such as "trace root, NeStat (NS) lookup, ping, etc." It would have been obvious because one of ordinary skill in the art would know that the disclosed "network diagnostic" functions comprises these specifically mentioned tools.

Regarding claim 12, Coley, discloses the method of claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using ping diagnostic tools to determine information about the source of the request for connection (Rejected under the same rationale as claim 11).

Regarding claim 13, Coley, discloses the method of claim 10, wherein using diagnostic tools to determine additional information about a source of the request for connection comprises using NS lookup diagnostic tools to determine information about the source of the request for connection (Rejected under the same rationale as claim 11).

Regarding claim 14, Coley, discloses the method of claim 10, further comprising forwarding the additional information to a system administrator via electronic mail (0046 – "send a electronic message").

Regarding claim 22, Coley, discloses the method of claim 15, further comprising using diagnostic tools to determine additional information about a source of the data packet (Rejected under the same rational as claim 11).

Regarding claim 23, Coley, discloses the method of claim 22, wherein using

diagnostic tools to determine additional information about a source of the data packet comprises using trace root diagnostic tools to determine additional information about the source of the data packet (Rejected under the same rational as claim 11).

Regarding claim 24, Coley, discloses the method of claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using ping diagnostic tools to determine additional information about the source of the data packet (Rejected under the same rationale as claim 11).

Regarding claim 25, Coley, discloses the method of claim 22, wherein using diagnostic tools to determine additional information about a source of the data packet comprises using NS lookup diagnostic tools to determine additional information about the source of the data packet (Rejected under the same rational as claim 11).

Regarding claim 26, Coley, discloses the method of claim 22, further comprising forwarding the additional information to a system administrator via electronic mail (Rejected under the same rational as claim 11).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436